I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

By: _____ Date: October 22, 2003

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applic. No. : 10/620,108
Applicant : Marcus Janke
Filed : July 15, 2003

Docket No. : S&ZIO020101
Customer No. : 24131

CLAIM FOR PRIORITY

Commissioner for Patents,
P.O. Box 1450, Alexandria, VA 22313-1450

Sir:

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119, based upon the German Patent Application 101 07 373.9, filed February 16, 2001.

A certified copy of the above-mentioned foreign patent application is being submitted herewith.

Respectfully submitted,

_____
For Applicant

MARKUS NOLFF
REG. NO. 37,006

Date: October 22, 2003

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

/av

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 101 07 373.9

Anmeldetag: 16. Februar 2001

Anmelder/Inhaber: Infineon Technologies AG, München/DE

Bezeichnung: Sicherheitsmodul mit flüchtigem Speicher zur Speicherung eines Algorithmuscodes

IPC: G 07 F 7/10

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 26. August 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

SL e

A 9161
03/00
EDV-L

—— SCHOPPE, ZIMMERMANN, STÖCKELER & ZINKLER ——

PATENTANWÄLTE

European Patent Attorneys
European Trademark Attorneys

Fritz Schoppe, Dipl.-Ing.
Tankred Zimmermann, Dipl.-Ing.
Ferdinand Stöckeler, Dipl.-Ing.
Franz Zinkler, Dipl.-Ing.

Telefon/Telephone 089/790445-0
Telefax/Facsimile 089/790 22 15
Telefax/Facsimile 089/74996977
e-mail: szsz_iplaw@t-online.de

Patentanwälte · Postfach 710867 · 81458 München

Infineon Technologies AG
St.-Martin-Str. 53

81669 München

Sicherheitsmodul mit flüchtigem Speicher zur Speicherung eines Algorithmuscodes

Beschreibung

Sicherheitsmodul mit flüchtigem Speicher zur Speicherung eines Algorithmuscodes

Die vorliegende Erfindung bezieht sich auf Sicherheitsmodule, wie sie beispielsweise bei Pay-TV-Anwendungen, Kreditkarten, Telefonkarten oder als TPM-Steckkarten, verwendet werden, und bezieht sich insbesondere auf eine Sicherung des für die Kommunikation zwischen Sicherheitsmodul und Terminal verwendeten Algorithmuscodes gegen äußere Attacken.

Mit der zunehmenden Verbreitung von bargeldlosem Zahlungsverkehr und der zunehmenden informationstechnischen Vernetzung bis in die einzelnen Haushalte, wie z. B. bei Pay-TV-Anwendungen, wächst der Bedarf nach Kryptographiealgorithmen, um digitale Signaturen, Authentifikationen und Verschlüsselungsaufgaben durchführen zu können. Bekannte Kryptographiealgorithmen umfassen asymmetrische Verschlüsselungsalgorithmen, wie z. B. den RSA-Algorithmus, symmetrische Verschlüsselungsverfahren, wie z. B. das DES-Verfahren, und auf elliptischen Kurven basierende Verfahren.

Um die durch die Kryptographiealgorithmen vorgeschriebenen Berechnungen im Alltag einerseits in akzeptabler Geschwindigkeit und andererseits für den Benutzer so bequem wie möglich durchführen zu können, werden Chipkarten, wie z. B. Smartcards oder Signaturkarten, eingesetzt, welche zur Implementierung des Kryptographiealgorithmus einen eigens vorgesehenen Kryptographieprozessor umfassen. Je nach Applikation bzw. Anwendung muß der Kryptographieprozessor in der Lage sein, Authentifikationen, Signaturen, Zertifizierungen und Ver- bzw. Entschlüsselungen nach verschiedenen Kryptographiealgorithmen vorzunehmen. Neben der Implementierung der Kryptographiealgorithmen befinden sich auf der Chipkarte gespeicherte, chipkartenspezifische Informationen, wie z. B. ein geheimer Schlüssel und in dem Fall einer Kreditkarte die Kreditkarten-

nummer, die Kontonummer und das Guthaben und in dem Fall einer Pay-TV-Smartcard eine Smartcard-ID, eine Kunden-ID und sonstige kundenspezifische Informationen. Dem Benutzer einer Chipkarte wird es durch die Chipkarte ermöglicht, auf einfache und effektive Weise bestimmte Transaktionen, wie z. B. eine Abbuchung, an extra vorgesehenen Terminals oder sonstigen Endgeräten, wie z. B. Pay-TV-Decodern, vorzunehmen. Hierbei sorgen die auf der Chipkarte implementierten Kryptographiealgorithmen für einen Schutz des Chipkartenverkehrs gegen kriminelle Übergriffe.

Um die Chipkarten-Terminal-Systeme gegen kriminelle Übergriffe zu schützen, werden zwischen Terminal und Chipkarte spezielle Protokolle verwendet, die beispielsweise eine gegenseitige Authentifikation und Ver- und Entschlüsselungen umfassen, die die in dem Kryptographieprozessor implementierten Kryptographiealgorithmen verwenden. Ein Problem bei herkömmlichen Chipkarten besteht darin, daß sich bei denselben die zum Einsatz kommenden Algorithmen für die geheimen Funktionen, wie z. B. zur Verschlüsselung, in Form einer festen Verdrahtung und/oder in gespeicherter Form fest auf der Chipkarte befinden und somit einem Ausspähen von potentiellen Angreifern ausgeliefert sind. Das Ausspähen von in Chipkarten implementierten Kryptographiealgorithmen durch einen Angreifer umfaßt beispielsweise das chemische Abtragen der Schaltungsstruktur des Kryptographieprozessors und das optische Analysieren der freigelegten Halbleiterstrukturen. Gelingt es einem Angreifer anhand der sich in seinem Besitz befindlichen Chipkarte an den in derselben implementierten Kryptographiealgorithmus zu gelangen, so wird es dem Angreifer aufgrund der Kenntnis des Kryptographiealgorithmus und damit durch die Ausführbarkeit desselben ermöglicht, bestimmte Attacken auf die Chipkarte auszuüben, um geheime Daten, wie z. B. den geheimen Schlüssel oder sonstige sicherheitskritische Daten der Chipkarte zu gewinnen. Bei Kenntnis des zugrunde liegenden Kryptographiealgorithmus haben die Attacken eine weitaus grö-

ßere Aussicht auf Erfolg, und folglich ist die Sicherheitskette des Chipkartenverkehrs gefährdet.

Dem Problem des Ausspähens wird bei herkömmlichen Chipkarten lediglich durch bestimmte Hardwareverfahren bzw. -technologien begegnet, wie z. B. durch das Hidden-Contact-Verfahren (Versteckte-Kontakte-Verfahren). Bei diesem Verfahren wird versucht, die optische Analyse abgetragener Halbleiterstrukturen und damit das Rückschließen auf die zugrundeliegende elektronische Schaltung durch versteckte Kontakte und durch eine Verwendung von speziellen Layout-Bibliotheken für die zugrundeliegenden Gatter, bei der sich verschiedene Gatter, wie z. B. ANDs und ORs, lediglich durch eine unterschiedliche Dotierung voneinander unterscheiden, zu verhindern. Diese hardwaremäßigen Verschleierungsmaßnahmen erhöhen zwar den Aufwand zum Herausfinden des zugrundeliegenden Kryptographiealgorithmus durch den potentiellen Angreifer, erhöhen aber andererseits den Schaltungs- und Entwurfsaufwand, die Chipfläche und damit die Kosten des Kryptographieprozessors bzw. der Chipkarte.

Eine Chipkarte mit erhöhter Sicherheit gegen Fremdattacken und einem reduzierten Schaltungsaufwand stellt gerade in Hinblick auf das hohe Marktpotential und die hohen Stückzahlen, in denen Chipkarten gefertigt werden, eine hohe Attraktivität für Chipkartenhersteller dar.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Sicherheitsmodul, ein Terminal und Verfahren zu schaffen, so daß ein sicherer Sicherheitsmodulverkehr gewährleistet werden kann.

Diese Aufgabe wird durch ein Sicherheitsmodul gemäß Anspruch 1, ein Terminal gemäß Anspruch 13 und ein Verfahren gemäß Anspruch 11, 14 oder 15 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß die Sicherheit eines Sicherheitsmoduls, wie z. B. einer Chipkarte, gegen Fremdattacken dadurch gesteigert werden kann, daß zumindest ein Teil des Algorithmuscodes nicht fest auf dem Sicherheitsmodul gespeichert wird, sondern daß dieser fehlende Teil des Algorithmuscodes vielmehr lediglich während der Kommunikation zwischen dem Terminal und dem Sicherheitsmodul in einem flüchtigen Speicher des Sicherheitsmoduls gespeichert wird, wobei der Algorithmuscode sicherheitskritische Funktionen, wie z. B. Abbuchungsfunktionen, oder Kryptographiealgorithmen umfaßt oder allgemein die Verarbeitung von Geheimnissen betrifft. Hierdurch wird wirksam verhindert, daß sich auf einem in der Gewalt eines potentiellen Angreifers befindlichen Sicherheitsmodul der vollständige Algorithmuscode befindet, und folglich wird es dem potentiellen Angreifer unmöglich gemacht, zur Ausspähung von geheimen Schlüsseln oder anderer geheimer Daten auf den Algorithmuscode zuzugreifen und denselben gemäß bestimmter Attacke-Verfahren auszuführen, wie z. B. unter Verwendung von Fault-Attacks (Fehlerattacken) oder Informations-Leck-Attacken. Anders ausgedrückt, wird es einem potentiellen Angreifer nahezu unmöglich gemacht, den Algorithmuscode, wie z. B. einen Verschlüsselungsalgorithmus, mißbräuchlich zu nutzen, da derselbe nicht dauerhaft in vollständiger Form auf dem Sicherheitsmodul gespeichert ist, und sich damit außerhalb des Einsatzes an einem entsprechenden Terminal nicht in dem Besitz des Angreifers befindet.

Erfindungsgemäß umfaßt ein Sicherheitsmodul, wie z. B. eine Chipkarte, ein TPM (Trusted Plattform Module) bzw. Sicherheitsplattformmodul in Form einer Computer-Steckkarte oder eine Smartcard, zur Verwendung mit einem Terminal neben einer Datenschnittstelle, die mit dem Terminal koppelbar ist, und von dem Terminal zumindest einen Teil des Algorithmuscodes oder den vollständigen Algorithmuscode empfängt, eine Energieschnittstelle, die Versorgungsenergie empfängt, und einen flüchtigen Speicher zum Speichern des über die Datenschnitt-

stelle empfangenen Teils des Algorithmuscodes oder des empfangenen vollständigen Algorithmuscodes, wobei der flüchtige Speicher mit der Energieschnittstelle gekoppelt ist, um mit Energie versorgt zu werden. Ein Prozessor führt den Algorithmuscode aus, um ein Algorithmuscodeergebnis zu erhalten, das zu dem Terminal lieferbar ist. Der nicht empfangene Rest des Algorithmuscodes kann beispielsweise in einem nicht-flüchtigen Speicher, wie z. B. einem ROM, des Sicherheitsmoduls gespeichert sein. Folglich befindet sich bei Fehlen einer ausreichenden Versorgungsenergie kein vollständiger Algorithmuscode in dem nicht-flüchtigen Speicher des Sicherheitsmoduls, und derselbe steht einem potentiellen Angreifer folglich nicht zur Ausführung zur Verfügung.

Ein zur Verwendung mit dem im vorhergehenden beschriebenen Sicherheitsmodul geeignetes Terminal, wie z. B. ein Bankautomat, ein Handy mit Kartenleser, ein Pay-TV-Decoder oder ein Computer mit einem Steckplatz für ein TPM, umfaßt beispielsweise eine Datenschnittstelle, die mit dem Sicherheitsmodul koppelbar ist, und die den Teil des Algorithmuscodes oder den vollständigen Algorithmuscode von dem Terminal zu dem flüchtigen Speicher des Sicherheitsmoduls sendet und das Algorithmuscodeergebnis von dem Sicherheitsmodul empfängt, sowie eine Energieschnittstelle, die die Versorgungsenergie zu dem Sicherheitsmodul liefert.

Gemäß einem speziellen Ausführungsbeispiel wird während einer Kommunikation zwischen dem Terminal und dem Sicherheitsmodul zunächst eine Authentifikation, wie z. B. eine Authentifikation nach dem Challenge- und -Response-Verfahren, zwischen dem Terminal und dem Sicherheitsmodul durchgeführt. Die Übertragung des Algorithmuscodes von dem Terminal zu dem Sicherheitsmodul erfolgt auf verschlüsselte und zertifizierte Weise, um einem Abhören bzw. Manipulieren der Kommunikationsverbindung zwischen dem Terminal und dem Sicherheitsmodul zu begegnen. In dem Terminal bzw. dem Sicherheitsmodul befinden sich hierzu geeignete Einrichtungen zur Durchführung einer

Authentifikation, einer Ver- bzw. Entschlüsselung und Zertifizierung bzw. Zertifikatsüberprüfung. Um die Sicherheit zu erhöhen, und um den Zugriff eines potentiellen Angreifers auf den übertragenen Teil des Algorithmuscodes wirksam zu verhindern, kann zusätzlich eine Überwachungseinrichtung in dem Sicherheitsmodul vorgesehen sein, die, falls vorbestimmte Sicherheitsbedingungen erfüllt werden, den flüchtigen Speicher löscht. Solche Sicherheitsbedingungen können die Unterbrechung, eine Unregelmäßigkeit und eine Schwankung der Versorgungsspannung und/oder des Prozessor- oder Systemtaktes oder anderer Betriebsparameter umfassen, wie sie durch Manipulation an dem Sicherheitsmodul bewirkt werden können, während dieses mit dem Terminal in Wechselwirkung steht. In dem Fall, daß die Überwachungseinrichtung nicht vorzeitig eine Löschung des Speichers bewirkt hat, wird der flüchtige Speicher und somit der gespeicherte Teil des Algorithmuscodes spätestens bei Beendigung der Kommunikation zwischen Terminal und Sicherheitsmodul bzw. bei Unterbrechung der Versorgungsenergie, wie z. B. durch Herausziehen bzw. Entfernen des Sicherheitsmoduls aus dem Terminal, gelöscht, wodurch dieser Teil des Algorithmuscodes einem potentiellen Angreifer nicht mehr zur Ausführung im Rahmen spezieller Attacken zur Verfügung steht.

Um die Angreifbarkeit des Systems weiter zu verringern, kann es vorgesehen sein, den Teil des Algorithmuscodes intermittierend in abgewandelter Form auf wiederholte Weise von dem Terminal zu dem Sicherheitsmodul zu übertragen, und hierbei jeweils den neu übertragenen, veränderten Teil des Algorithmuscodes anstatt des alten gespeicherten Teils des Algorithmuscodes in dem flüchtigen Speicher zu speichern. Hierdurch sind Wechsel eines Kryptographiealgorithmus während der Kommunikation zwischen Terminal und Sicherheitsmodul, wie z. B. bei Pay-TV-Anwendungen, aber auch Algorithmuscodewechsel jeweils bei Initialisierung einer Terminal-Sicherheitsmodul-Kommunikation, wie z. B. bei Kreditkarten, möglich, wodurch es einem potentiellen Angreifer weiter erschwert wird, sich

auf den verwendeten Algorithmuscode einzustellen, bzw. denselben zu eroieren.

Neben dem Bewahren des Algorithmuscodes des Sicherheitsmoduls vor einem Ausspähen durch einen potentiellen Angreifer besteht ein weiterer Vorteil der vorliegenden Erfindung darin, daß sie auf eine Vielzahl von Anwendungsgebieten, wie z. B. EC-Karten, Kreditkarten, Multiapplikationskarten oder Pay-TV-Smartcards, anwendbar ist. Je nach Applikation enthält der von dem Sicherheitsmodul empfangene Algorithmuscode bzw. Sicherheitsfunktionscode Teile eines Codes für sicherheitskritische Funktionen oder einen oder mehrere Kryptographiealgorithmen des Sicherheitsmoduls. Für Chipkartenhersteller oder Hersteller von Sicherheitsmodulen bedeutet die vielseitige Anwendbarkeit sowie die erhöhte Sicherheit gegen potentielle Angriffe eine erhöhte Marktakzeptanz und somit einen größeren Marktanteil. Zudem wird die Sicherheit des Sicherheitsmoduls auf kostengünstige Weise erhöht, da die erhöhte Sicherheit durch softwaremäßiges Laden des flüchtigen Speichers erzielt wird. Die herkömmlichen und aufwendigen Hardwaremaßnahmen zum Schutz des Algorithmuscodes vor potentiellen Angreifern, wie sie im vorhergehenden beschrieben wurden, können entweder zusätzlich vorgenommen oder aber durch kostengünstigere Hardwareverfahren ersetzt werden, da sich die sicherheitskritischen Funktionen oder der zugrundeliegende Kryptographiealgorithmus des Sicherheitsmoduls nicht dauerhaft auf der Chipkarte befinden.

Weiterbildungen und weitere alternative Ausführungsbeispiele der vorliegenden Erfindung sind in den beiliegenden Unteransprüchen definiert.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

Fig. 1 ein schematisches Diagramm, das den Ablauf während der Kommunikation einer Chipkarte mit einem Terminal gemäß der vorliegenden Erfindung veranschaulicht;

Fig. 2 ein Blockdiagramm eines Chipkartenaufbaus gemäß einem Ausführungsbeispiel der vorliegenden Erfindung; und

Fig. 3 einen Terminalaufbau gemäß einem Ausführungsbeispiel der vorliegenden Erfindung.

Es wird darauf hingewiesen, daß sich die folgende detaillierte Beschreibung bestimmter Ausführungsbeispiele der vorliegenden Erfindung lediglich exemplarisch auf Chipkarten-Anwendungen bezieht, und daß die vorliegende Erfindung statt dessen auch auf andere Sicherheitsmodule anwendbar ist, wie z.B. auf TPMs in Form von Steckkarten, wobei die folgende Beschreibung ohne weiteres auf solche Anwendungen übertragbar ist. Dementsprechend bezieht sich die folgende Beschreibung auch lediglich exemplarisch auf Terminals für Chipkarten, wie z.B. Bankautomaten, obwohl ein Terminal der vorliegenden Erfindung bei anderen Anwendungsgebieten beispielsweise auch ein Computer sein kann, in dessen Steckplätzen sich ein TPM befindet, oder ein Handy, in dessen Kartenleser sich eine Smartcard befindet, oder das Terminal allgemein jede Vorrichtung sein kann, die in der Lage ist, mit dem Sicherheitsmodul zu kommunizieren.

Es wird zunächst auf Fig. 1 Bezug genommen, die den Ablauf während einer Kommunikation zwischen einem Terminal und einer Chipkarte darstellt, wie er sich beispielsweise ergibt, wenn eine Chipkarte in ein Terminal eingeführt wird. In dem Fall des gebührenpflichtigen Rundfunks kann die Chipkarte beispielsweise eine Pay-TV-Smartcard und das Terminal das jeweilige Endgerät bzw. der Decoder eines Pay-TV-Kunden sein. In

dem Fall, daß die Chipkarte eine Kreditkarte ist, ist das Terminal beispielsweise ein Bankautomat.

In Fig. 1 sind die Chipkarte 10 und das Terminal 20 nebeneinander durch Rechtecke mit abgerundeten Ecken gezeigt. Darunter sind schematisch durch Pfeile und Blöcke in der Reihenfolge ihres Auftretens von oben nach unten die verschiedenen Schritte dargestellt, die während der Kommunikation bzw. Wechselwirkung der Chipkarte 10 mit dem Terminal 20 durchgeführt werden. Die Pfeilrichtungen geben die Richtungen der Datenflüsse an, in die Daten gesendet werden, während die Blöcke Maßnahmen darstellen, die in der Chipkarte 10 durchgeführt werden.

Die in Fig. 1 dargestellten Schritte setzen voraus, daß bereits eine Kommunikation zwischen dem Terminal und der Chipkarte möglich ist, was beispielsweise nach Einfügen der Chipkarte in das Terminal der Fall sein kann, wobei das Terminal 20 ein Kontaktlos- oder ein Kontakt-Terminal sein kann, und die Kommunikationsverbindung somit kontaktlos oder über einen Kontakt stattfinden kann. Zur Kommunikation ist es ferner erforderlich, daß die Chipkarte 10 von dem Terminal 20 mit Energie versorgt wird, was ebenfalls entweder kontaktlos über eine elektromagnetische Strahlung oder über einen Kontakt durchgeführt werden kann. Nach der Herstellung der Kommunikationsverbindung zwischen dem Terminal 20 und der Chipkarte 10 sowie der Versorgung der Chipkarte 10 mit Versorgungsenergie können zunächst Schritte zur Initialisierung durchgeführten werden, wie z. B. die gegenseitige Vereinbarung des maßgebenden Protokolls usw.

Nach den Schritten (nicht gezeigt) zur Energieversorgung der Chipkarte 10, zur Herstellung der Kommunikationsverbindung sowie zur Initialisierung der Kommunikation zwischen dem Terminal 20 und der Chipkarte 10 wird in einem Schritt 30 eine gegenseitige Authentifikation zwischen dem Terminal 20 und der Chipkarte 10 durchgeführt, wie z. B. eine Authentifikati-

on nach dem Challenge-Und-Response-Verfahren. Die gegenseitige Authentifikation kann beispielsweise eine PIN- (Personal Identifikation Number = Personenkennzahl) Eingabe durch den Kartenbenutzer umfassen, wobei zur gegenseitigen Authentifikation 30 beispielsweise auf der Chipkarte 10 gespeicherte chipkartenspezifische Daten, wie z. B. eine Chipkartenidentifikationsnummer und eine Personenkennzahl, in Verbindung mit einem auf der Chipkarte gespeicherten Chipkartenschlüssel und einem auf der Chipkarte gespeicherten Authentifizierungscode, der einen Kryptographiealgorithmus, wie z. B. einen symmetrischen oder einen asymmetrischen kryptographischen Algorithmus, darstellt, verwendet werden können. Die Authentifikation dient dazu, um sicherzustellen, daß nur zugelassene Chipkarten mit zugelassenen Terminals kommunizieren können. Ergibt die Authentifikation einen Fehler, so wird die Kommunikationsverbindung abgebrochen.

Nach erfolgreicher gegenseitiger Authentifikation 30 sendet das Terminal 20 in einem Schritt 40 einen Teil des Algorithmuscodes verschlüsselt und zertifiziert an die Chipkarte 10. Die Verschlüsselung des übertragenen Teils des Algorithmuscodes schützt die Übertragung vor einem Abhören durch einen potentiellen Angreifer, während die Zertifizierung in dem Terminal 20 der Chipkarte 10 eine Garantie über die Herkunft des übertragenen Teils des Algorithmuscodes geben soll. Die Chipkarte 10 umfaßt zur Entschlüsselung des übertragenen Teils des Algorithmuscodes und zur Überprüfung des Zertifikats ebenso wie zur Durchführung der gegenseitigen Authentifikation 30 geeignete Authentifikations-, Entschlüsselungs- und Zertifikatsüberprüfungseinrichtungen, die sich aus einem Teil der Hardware und aus in einem nicht-flüchtigen Speicher der Chipkarte gespeicherten Codes, wie z. B. dem Authentifikationscode, zusammensetzen. Die Kryptographiealgorithmen, die der gegenseitigen Authentifikation 30 und der Verschlüsselung und Zertifizierung 40 zugrundeliegen, können symmetrische oder asymmetrische Kryptographieverfahren umfassen, wie z. B.

den RSA- oder den DES-Algorithmus, oder einen beliebigen anderen Kryptographiealgorithmus.

Falls die Zertifikatsüberprüfung ergibt, daß die Echtheit des Zertifikats fehlt, wird die Kommunikation zwischen dem Terminal 20 und der Chipkarte 10 abgebrochen, und es kann vorgesehen sein, daß die Chipkarte 10 für eine vorbestimmte Zeit keine Verarbeitungen mehr durchführt. Hierdurch wird vermieden, daß ein potentieller Angreifer die Kommunikationsverbindung zwischen dem Terminal 20 und der Chipkarte 10 anzapft und einen „falschen" Code in den flüchtigen Speicher der Chipkarte 10 einspeist, der bei Ausführung durch die Chipkarte 10 beispielsweise die Ausgabe geheimer, auf der Chipkarte 10 gespeicherter Daten bewirken könnte.

In einem Schritt 50 wird, wenn die Zertifikatsüberprüfung die Echtheit des Zertifikats ergab, der übertragene Teil des Algorithmuscodes in einem flüchtigen Speicher der Chipkarte 10 in entweder verschlüsselter oder entschlüsselter Form gespeichert. Je nach verschlüsselter oder entschlüsselter Speicherung wird der Algorithmuscode vor der Speicherung oder vor der Ausführung durch einen Kryptographieprozessor auf der Chipkarte 10 entschlüsselt. Der Algorithmuscode, von dem ein Teil in dem Schritt 40 übertragen wird, kann den Programmcode eines oder einer Mehrzahl von sicherheitskritischen Funktionen der Chipkarte 10, wie z. B. eine Ab- oder Aufbuchungsfunktion zum Be- oder Entladen der Chipkarte 10, oder den Programmcode zur Durchführung eines während des weiteren Kommunikationsablaufes erforderlichen kryptographischen Algorithmus umfassen, wie z. B. ,aber nicht ausschließlich, ein symmetrisches oder asymmetrisches Kryptographieverfahren, einen RSA-Algorithmus, eine Verschlüsselung nach dem DES-Standard, ein Elliptisches-Kurven-Verfahren oder einen anderen geheimen Algorithmus. In dem Fall einer Pay-TV-Anwendung umfaßt der Algorithmuscode beispielsweise Informationen bezüglich der Entschlüsselung der Fernsehdaten eines gebührenpflichtigen Programmes, wie z. B. die Repermutation der Bild-

zeilen eines Bildes der Fernsehdaten. Folglich befindet sich der zu schützende Algorithmuscode in vollständiger Form lediglich zur Laufzeit der Kommunikation zwischen dem Terminal 20 und der Chipkarte 10 auf der Chipkarte 10.

In einem Schritt 60 wird der sich nun in vollständiger Form auf der Chipkarte 10 befindliche Algorithmuscode angewendet und von einem auf der Chipkarte 10 befindlichen Prozessor ausgeführt. In dem im vorhergehenden erwähnten Pay-TV-Beispiel führt der Prozessor der Chipkarte 10 beispielsweise die Repermutation der Bildzeilen der Fernsehbilder anhand des gespeicherten Algorithmuscodes durch. Bei einer Debbit-Anwendung der Chipkarte 10, wie z. B. bei Telefonkarten, wird beispielsweise der eine Ab- bzw. Aufbuchungsfunktion angebende Algorithmuscode verwendet, um ein auf der Chipkarte 10 befindliches Guthaben ab- oder aufzubuchen. Bei Kreditanwendungen umfaßt der Schritt 60 beispielsweise die Ausführung des einen kryptographischen Algorithmus angebenden Algorithmuscodes durch einen Kryptographieprozessor der Chipkarte 10, um beispielsweise Überweisungsaufträge zu erteilen.

In einem Schritt 70 wird der in dem flüchtigen Speicher gespeicherte Teil des Algorithmuscodes wieder gelöscht. Die Löschung des Algorithmuscodes kann beispielsweise durch das Herausnehmen der Chipkarte 10 aus dem Terminal 20 durch den Kartenbenutzer und damit das Unterbrechen der Versorgungsenergiezufuhr von dem Terminal 20 zu der Chipkarte 10 bewirkt werden. Um die Versuche von potentiellen Angreifern, den flüchtigen Speicher, wie z. B. einem RAM, vor einem Verlust des gespeicherten Teils des Algorithmuscodes zu schützen, zu verhindern, wodurch dieselben in den Besitz des vollständigen Algorithmuscodes kämen, kann auf der Chipkarte 10 eine spezielle Überwachungseinrichtung vorgesehen sein, die eine aktive Löschung des flüchtigen Speichers der Chipkarte 10 auch dann bewirkt, falls eine Überwachung ergibt, daß spezielle Sicherheitsbedingungen erfüllt sind, wie z. B. die Unterbrechung des Systemtaktes, die Unterbrechung der Versorgungsenergiezu-

fuhr oder sonstige Anzeichen für einen möglichen Angriff, wie z. B. Spannungsschwankungen oder dergleichen. Folglich befindet sich der Algorithmuscode nach dem Einsatz der Chipkarte 10 in dem Terminal 20 oder einer Störung des Kommunikationsablaufes nicht mehr auf der Chipkarte 10, und ist somit nicht mehr den potentiellen Angriffen und dem Ausspähen durch potentieller Angreifer ausgeliefert. Ein Angreifer, der im Besitz der Chipkarte ist, kann keine Sicherheitsberechnungen basierend auf dem vollständigen Algorithmuscode ausführen, da sich derselbe nicht vollständig in seinem Zugriffsbereich befindet. Das Ausspähen von Schlüsseln oder Algorithmen wird somit wirksam unterbunden.

Nachdem bezugnehmend auf Fig. 1 der Ablauf während der Kommunikation einer Chipkarte mit einem Terminal beschrieben worden ist, werden im folgenden zunächst verschiedene Möglichkeiten beschrieben, welche Teile eines Algorithmuscodes von dem Terminal zu dem flüchtigen Speicher der Chipkarte übertragen werden. In dem Fall, daß der Algorithmuscode den Programmcode eines geheimen, noch nicht bekannten Kryptographiealgorithmusses enthält, kann es beispielsweise vorteilhaft sein, den Algorithmuscode vollständig von dem Terminal in den flüchtigen Speicher der Chipkarte zu übertragen, wodurch dieser geheime Kryptographiealgorithmus wirksam vor dem Ausspähen durch einen potentiellen Angreifer geschützt wäre.

In dem Fall, daß der übertragene Teil des Algorithmuscodes einen Teil eines Programmcodes für einen bekannten Kryptographiealgorithmus enthält, umfaßt der übertragene Teil des Programmcodes beispielsweise Speicheradressen, in denen die der kryptologischen Berechnung zugrundeliegenden Berechnungskomponenten gespeichert sind, wodurch wirksam vermieden wird, daß ein potentieller Angreifer, der im Besitz der Chipkarte ist, die auf diesem Kryptographiealgorithmus basierenden Sicherheitsberechnungen durchführen kann, da zur Ausführung des Programmcodes bzw. für die hierzu erforderlichen Speicher-

zugriffe durch den Prozessor der Chipkarte die erforderlichen Speicheradressen fehlen.

In dem Fall eines bekannten Kryptographiealgorithmusses können in dem übertragenen Teil des Algorithmuscodes Sprungadressen umfaßt sein, die entweder als Startadresse auf den Anfang eines bestimmten Programmcodes oder als bedingte oder unbedingte Programmsprünge auf die Anfänge bestimmter Teilroutinen zeigen. Ohne Kenntnis dieser Sprungadressen wird es einem Angreifer sehr schwierig gemacht, die sich in seiner Gewalt befindliche Chipkarte auszuspähen.

Bei einem speziellen Beispiel können auf der Chipkarte 10 eine Mehrzahl von Programmcodes für verschiedene Kryptographiealgorithmen vorgesehen sein, wobei der übertragene Teil des Algorithmuscodes eine Anfangsadresse eines bestimmten der verschiedenen Kryptographiealgorithmenprogrammcodes enthält, der gerade von dem Terminal ausgewählt worden ist. Das Terminal wählt beispielsweise für jeden neuen Chipkarte-Terminal-Kommunikationsvorgang einen neuen Kryptographiealgorithmus der Mehrzahl von Kryptographiealgorithmen aus, oder die Auswahl wird während eines Kommunikationsvorganges dynamisch mehrmals neu durchgeführt, um den ausgewählten Kryptographiealgorithmus dynamisch zu verändern.

Es kann ferner vorgesehen sein, daß der übertragene Teil des Algorithmuscodes Startadressen, Sprungadressen oder Speicheradressen eines Programmcodes enthält, der zur Abbuchung oder Aufbuchung oder für sonstige sicherheitskritische Funktionen der Chipkarte erforderlich ist. Ferner ist es möglich, daß die in Fig. 1 gezeigten Schritte 40, 50 und 60 wiederholt werden, wobei der übertragene Teil des Algorithmuscodes auf vorbestimmte Weise geändert wird. Bei jedem Durchgang wird der alte in dem flüchtigen Speicher der Chipkarte gespeicherte Teil des Algorithmuscodes durch den neu übertragenen Teil des Algorithmuscodes überschrieben, der daraufhin von dem Prozessor der Chipkarte ausgeführt wird. Durch diese dynami-

sche Modifizierung des in dem flüchtigen Speicher gespeicherten Teils des Algorithmuscodes wird eine zusätzliche Sicherheit erzielt.

Bezugnehmend auf Fig. 2 und Fig. 3 werden nun im folgenden mögliche Ausführungsbeispiele für den Aufbau einer Chipkarte bzw. eines Terminals beschrieben. Fig. 2 zeigt ein Blockschaltbild einer Chipkarte, die allgemein mit 100 angezeigt wird. Die Chipkarte 100 umfaßt eine Datenschnittstelle 110, eine Energieschnittstelle 120, einen RAM 130, einen Prozessor 140 und einen ROM 150. Die Datenschnittstelle 110 ist beispielsweise über eine kontaktlose Kopplung oder über einen Kontakt mit einem Terminal (nicht gezeigt) koppelbar und ist in der Lage, Daten von der Chipkarte zu dem Terminal zu senden und umgekehrt Daten von dem Terminal zu empfangen. Die Datenschnittstelle 110 ist mit dem Prozessor 140 verbunden, wodurch die zu sendenden und die empfangenen Daten von bzw. zu dem Prozessor 140 übertragen werden können. Die Energieschnittstelle 120 ist ebenfalls mit dem Terminal koppelbar, um von dem Terminal Versorgungsenergie in Form von beispielsweise elektromagnetischer Energie oder einer Versorgungsspannung, zu erhalten. Die Energieschnittstelle 120 verteilt die Versorgungsenergie auf den Prozessor 140 und den RAM 130 auf.

Der Prozessor 140 besteht beispielsweise aus einer CPU (nicht gezeigt) und mehreren Kryptocoprozessoren (nicht gezeigt), die von der CPU gesteuert werden und für spezielle Berechnungen ausgestaltet sind, die für den einen oder die mehreren Kryptographiealgorithmen, die in der Chipkarte 100 implementiert sind, erforderlich sind, wie z. B. modulare oder arithmetische Berechnungen. Die CPU führt neben der Steuerung der Kryptocoprozessoren ferner die Kommunikation über die Datenschnittstelle 110 mit dem Terminal und Speicherzugriffe auf den mit dem Prozessor 140 verbundenen ROM 150 aus. Auf dem ROM 150 befinden sich beispielsweise chipkartenspezifische Informationen, wie z. B. eine Chipkartenidentifikationsnum-

mer, eine Personenkennzahl, eine Kontonummer, ein Guthaben oder dergleichen.

Die CPU des Prozessors 140 übernimmt die Aufgaben zur Initialisierung einer Kommunikation eines Terminals mit der Chipkarte 100, zur Authentifikation sowie zur Entschlüsselung und Zertifikatsüberprüfung bei Empfang des erfindungsgemäß übertragenen Teils des Algorithmuscodes, wobei ein hierzu erforderlicher Programmcode in dem ROM 150 gespeichert sein kann. Zur Durchführung der weiteren Kommunikation mit dem Terminal, wie z. B. zur Durchführung sicherheitsspezifischer Funktionen, wie z. B. dem Abheben eines in dem ROM 150 gespeicherten Guthabens, oder eines kryptographischen Algorithmus, um eine Kontobuchungstransaktion auszuführen, wird die CPU des Prozessors 140 durch einen Programmcode programmgesteuert, welcher sich während einer Kommunikation der Chipkarte 100 mit dem Terminal erfindungsgemäß zumindest teilweise in dem mit dem Prozessor 140 verbundenen RAM 130 und andernfalls entweder überhaupt nicht oder nur teilweise in dem ROM 150 auf der Chipkarte 100 befindet. Ein potentieller Angreifer, der im Besitz der Chipkarte 100 ist, kann folglich, wie es im vorhergehenden beschrieben wurde, die Sicherheitsberechnungen durch den Prozessor 140 nicht ausführen, da Teile des Algorithmuscodes fehlen und erst bei Kommunikation der Chipkarte mit dem Terminal in dem flüchtigen Speicher 130 gespeichert werden.

In Fig. 3 ist ein Blockdiagramm gezeigt, das den Terminalaufbau gemäß einem Ausführungsbeispiel der vorliegenden Erfindung zeigt. Das Terminal, das allgemein mit 200 angezeigt ist, umfaßt eine Datenschnittstelle 210, eine Energieschnittstelle 220, einen mit der Datenschnittstelle 210 und der Energieschnittstelle 220 verbundenen Prozessor 230 und einen mit dem Prozessor 230 verbundenen Speicher 240. Die Datenschnittstelle 210 ist mit der Datenschnittstelle einer entsprechenden Chipkarte koppelbar, um einen Datenaustausch zwischen dem Terminal 200 und der Chipkarte (nicht gezeigt)

durchzuführen. Die Energieschnittstelle 220 ist ebenfalls mit einer Energieschnittstelle der entsprechenden Chipkarte koppelbar, um Versorgungsenergie zu derselben zu liefern. Der Prozessor 230 steuert beispielsweise den Ablauf während der Kommunikation des Terminals 200 mit der Chipkarte und führt beispielsweise die Initialisierung, Authentifikation, die Verschlüsselung des zu übertragenden Algorithmuscodes, der in dem Speicher 240 gespeichert ist, die Zertifizierung desselben und die Übertragung des verschlüsselten und zertifizierten Algorithmuscodes zu der Datenschnittstelle 210 für eine Übertragung an die Chipkarte durch.

Es sei darauf hingewiesen, daß der Speicher 240 den Algorithmuscode beispielweise bereits in verschlüsselter Form enthalten kann, so daß der Prozessor 230 denselben nicht verschlüsseln muß, und derselbe weder in dem Speicher 240 noch anderswo in Klartext vorliegt.

Bezugnehmend auf die vorhergehende Beschreibung wird darauf hingewiesen, daß sich dieselbe lediglich auf spezielle Ausführungsbeispiele bezog. Die gegenseitige Authentifikation und die Verschlüsselung des übertragenen Teils des Algorithmuscodes sowie die Zertifizierung können beispielsweise bei speziellen Anwendungen weggelassen werden. Durch die erfindungsgemäße Speicherung zumindest eines Teils des Algorithmuscodes in einem flüchtigen Speicher der Chipkarte allein wird es einem potentiellen Angreifer sehr schwer gemacht, sicherheitskritische Funktionen der Chipkarte, wie z. B. Verschlüsselungsalgorithmen und Zugriffsfunktionen auf chipkartenspezifische Informationen, wie z. B. ein Guthaben, usw., auszuführen, da diese nicht dauerhaft auf der Chipkarte gespeichert sind und sich damit nicht in Besitz des potentiellen Angreifers befinden, sondern dieselben vielmehr bei Wegfall des Versorgungsenergieempfangs verloren gehen. Der Versuch, den flüchtigen Speicher vor Verlust der Funktion zu schützen, gestaltet sich als äußerst diffizil und kann als praktisch nicht realisierbar gelten.

Es wird ferner darauf hingewiesen, daß die erfindungsgemäßen Verfahren, das erfindungsgemäße Terminal und die erfindungsgemäße Chipkarte auf verschiedene Arten und Weisen implementiert sein können. Die entsprechenden Schritte bzw. Einrichtungen können mittels Software, Firmware oder Hardware in Verbindung mit nicht-flüchtigen Speichern implementiert sein. Zudem soll der Begriff Chipkarte, wie er im vorhergehenden verwendet wurde, nicht auf die Form einer Karte begrenzt sein, sondern vielmehr sollen auch alle anderen Formen von Chipträgern umfasst sein, die auf ähnliche Weise verwendet werden.

Eine derzeitige Realisierungsmöglichkeit der vorliegenden Erfindung besteht beispielsweise in dem Prozessor der Produktfamilie SLE66CX320P der Firma Infineon AG, der es durch eine MMU (MMU = Memory Management Unit = Speicherverwaltungseinheit) ermöglicht, einen in einem RAM gespeicherten Code auszuführen, indem dieselbe Speicherzugriffe auf den RAM steuert. Im einfachsten Fall würde bereits durch das Übertragen verschlüsselter Sprungadressen oder Speicheradressen von dem Terminal zu der Chipkarte wirksam verhindert werden, daß von einem potentiellen Angreifer ein „nativ-code" bzw. Maschinencode geladen werden kann. Ein Angreifer könnte bereits bei einer solchen einfachen Realisierung der vorliegenden Erfindung die Sicherheitsberechnungen in der Chipkarte nicht ausführen, da die Sprungadressen und damit die Abläufe unbekannt wären. Durch das Erstellen einer Application-Note kann dem Kunden eines solchen Bausteins diese Idee vermittelt werden und hierdurch die Sicherheit der Anwendung bei entsprechender Umsetzung in der Controller-Software der Chipkarte und in der Terminal-Software erhöht werden.

Potentiellen Angreifern, die im Besitz einer erfindungsgemäßen Chipkarte sind, liegen nur die geschützten Daten vor, sie können aber weder eine Verrechnung initiieren, noch den Algorithmuscode exakt bestimmen. In Kombination mit gesicherten

Terminals und intelligenten Zugriffsschutzmechanismen betreffend der Nachladbarkeit von Programmteilen liefert die vorliegende Erfindung somit eine sehr hohe Sicherheit.

Patentansprüche

1. Sicherheitsmodul zur Verwendung mit einem Terminal, mit

einer Datenschnittstelle (110), die mit einem Terminal koppelbar ist, zum Empfangen zumindest eines Teils eines Algorithmuscodes oder des vollständigen Algorithmuscodes von dem Terminal;

einer Energieschnittstelle (120) zum Empfangen von Versorgungsenergie;

einem flüchtigen Speicher (130) zum Speichern des über die Datenschnittstelle (110) empfangenen Teils des Algorithmuscodes oder des vollständigen Algorithmuscodes, wobei der flüchtige Speicher (130) mit der Energieschnittstelle (120) gekoppelt ist, um mit Energie versorgt zu werden; und

einem Prozessor (140) zum Ausführen des Algorithmuscodes, um ein Algorithmuscodeergebnis zu erhalten, das zu dem Terminal lieferbar ist.

2. Sicherheitsmodul, das ferner folgendes Merkmal aufweist:

einen nicht-flüchtigen Speicher (150), in dem der nicht empfangene Rest des Algorithmuscodes gespeichert ist.

3. Sicherheitsmodul gemäß Anspruch 1 oder 2, das ferner folgendes Merkmal aufweist.

eine Einrichtung (140, 150) zum Durchführen einer Authentifikation zwischen dem Terminal und dem Sicherheitsmodul.

4. Sicherheitsmodul gemäß einem der Ansprüche 1 bis 3, bei dem die Datenschnittstelle (110) angeordnet ist, um von dem Terminal den Teil des Algorithmuscodes oder den vollständigen Algorithmuscode in verschlüsselter Form und/oder ein Zertifi-

kat zu erhalten, wobei das Sicherheitsmodul ferner folgende Merkmale aufweist:

eine Einrichtung (140, 150) zum Entschlüsseln des Teils des verschlüsselten Algorithmuscodes oder des verschlüsselten vollständigen Algorithmuscodes; und

eine Einrichtung (140, 150) zum Überprüfen des Zertifikats und zum Verhindern des Ausführens des Algorithmuscodes bei fehlender Echtheit des Zertifikats.

5. Sicherheitsmodul gemäß einem der Ansprüche 1 bis 4, das ferner folgendes Merkmal aufweist:

eine Speicherverwaltungseinheit zum Steuern von Speicherzugriffen des Prozessors, wobei der übertragenen Teil des Algorithmuscodes Adressen des Algorithmuscodes enthält.

6. Sicherheitsmodul gemäß einem der Ansprüche 1 bis 5, das ferner folgendes Merkmal aufweist:

eine Einrichtung zum Überwachen einer vorbestimmten Sicherheitsbedingung und zum Löschen des flüchtigen Speichers (130), falls die vorbestimmte Sicherheitsbedingung erfüllt ist, wobei die Sicherheitsbedingung aus einer Mehrzahl von Bedingungen ausgewählt ist, die eine Unterbrechung, eine Unregelmäßigkeit und eine Schwankung der Versorgungsspannung und eines Systemtaktes und weiterer Betriebsparameter umfaßt.

7. Sicherheitsmodul gemäß einem der Ansprüche 1 bis 6, bei dem der Algorithmuscode einen Programmcode aufweist, der zur Ausführung einer Aufgabe vorgesehen ist, die aus einer Gruppe ausgewählt ist, die einen symmetrischen Kryptographiealgorithmus, einen asymmetrischen Kryptographiealgorithmus, einen RSA-Algorithmus, ein Kryptographieverfahren nach dem DES-Standard, ein Elliptisches-Kurven-Verfahren und eine Zugriffsfunktion zum Zugreifen und eine Zugriffsfunktion zum

Verändern eines auf dem Sicherheitsmodul gespeicherten Werts umfaßt.

8. Sicherheitsmodul gemäß einem der Ansprüche 1 bis 7, bei dem der empfangene Teil des Algorithmuscodes eine Startadresse des Algorithmuscodes, Speicheradressen von für die Ausführung des Algorithmuscodes erforderlichen Berechnungskomponenten oder Sprungadressen des Algorithmuscodes aufweist.

9. Sicherheitsmodul gemäß einem der Ansprüche 1 bis 8, bei dem der flüchtige Speicher (130) angeordnet ist, um den gespeicherten Teil des Algorithmuscodes oder den gespeicherten vollständigen Algorithmuscode mit einem neu empfangenen, veränderten Teil des Algorithmuscodes zu überspeichern.

10. Sicherheitsmodul gemäß einem der Ansprüche 1 bis 9, wobei das Sicherheitsmodul als Chipkarte ausgeführt ist.

11. Verfahren zum Berechnen eines Algorithmuscodeergebnisses unter Verwendung eines Sicherheitsmoduls, mit folgenden Schritten:

Empfangen (40) zumindest eines Teils des Algorithmuscodes oder des vollständigen Algorithmuscodes;

flüchtiges Speichern (50) des Teils des Algorithmuscodes oder des vollständigen Algorithmuscodes in einem flüchtigen Speicher (130) des Sicherheitsmoduls;

Ausführen (60) des Algorithmuscodes auf dem Sicherheitsmodul, um ein Algorithmuscodeergebnis zu erhalten;

Liefern (60) des Algorithmuscodeergebnisses zu dem Terminal; und

Löschen (70) des flüchtigen Speichers (130).

12. Verfahren gemäß Anspruch 11, bei dem der Schritt des Löschens (70) das Entfernen des Sicherheitsmoduls von dem Terminal aufweist.

13. Terminal zur Verwendung mit einem Sicherheitsmodul, mit folgenden Merkmalen:

einer Datenschnittstelle (210), die mit dem Sicherheitsmodul (100) koppelbar ist, zum Senden zumindest eines Teils eines Algorithmuscodes oder des vollständigen Algorithmuscodes von dem Terminal zu einem flüchtigen Speicher (130) des Sicherheitsmoduls (100) und zum Empfangen eines Algorithmuscodeergebnisses von dem Sicherheitsmodul; und

einer Energieschnittstelle (220) zum Liefern von Versorgungsenergie zu dem Sicherheitsmodul.

14. Verfahren zum Steuern eines Sicherheitsmoduls unter Verwendung eines Terminals, um von dem Sicherheitsmodul ein Algorithmuscodeergebnis zu erhalten, mit folgenden Schritten:

Liefern von Versorgungsenergie zu dem Sicherheitsmodul;

Senden (60) zumindest eines Teils eines Algorithmuscodes oder des vollständigen Algorithmuscodes von dem Terminal zu einem flüchtigen Speicher des Sicherheitsmoduls; und

Empfangen (60) des Algorithmuscodeergebnisses von dem Sicherheitsmodul.

15. Verfahren zur Kommunikation zwischen einem Sicherheitsmodul und einem Terminal, mit folgenden Schritten:

Übertragen (40) zumindest eines Teils eines Algorithmuscodes oder des vollständigen Algorithmuscodes von dem Terminal zu dem Sicherheitsmodul;

flüchtiges Speichern (50) des Teils des Algorithmuscodes oder des vollständigen Algorithmuscodes in einem flüchtigen Speicher (130) des Sicherheitsmoduls;

Ausführen (60) des Algorithmuscodes auf dem Sicherheitsmodul, um ein Algorithmuscodeergebnis zu erhalten;

Liefern (60) des Algorithmuscodeergebnisses zu dem Terminal; und

Löschen (70) des flüchtigen Speichers (130).

16. Verfahren gemäß Anspruch 15, das ferner folgenden Schritt aufweist:

wiederholtes Übertragen einer einer Mehrzahl von unterschiedlichen Fassungen des Teils des Algorithmuscodes oder des vollständigen Algorithmuscodes; und

Überspeichern des gespeicherten Teils des Algorithmuscodes oder des vollständigen gespeicherten Algorithmuscodes durch die wiederholt übertragene Fassung des Teil des Algorithmuscodes oder des vollständigen Algorithmuscodes.

Zusammenfassung

Sicherheitsmodul mit flüchtigem Speicher zur Speicherung eines Algorithmuscodes

Ein Sicherheitsmodul (100) zur Verwendung mit einem Terminal umfaßt eine Datenschnittstelle(110), die mit einem Terminal koppelbar ist, zum Empfangen zumindest eines Teils eines Algorithmuscodes oder des vollständigen Algorithmuscodes von dem Terminal sowie eine Energieschnittstelle (120) zum Empfangen von Versorgungsenergie. Ein flüchtiger Speicher (130), der mit der Energieschnittstelle (120) gekoppelt ist, um mit Energie versorgt zu werden, speichert den über die Datenschnittstelle empfangenen Teil des Algorithmuscodes oder den vollständigen Algorithmuscode, wobei ein Prozessor (140) den Algorithmuscode ausführt, um ein Algorithmuscodeergebnis zu erhalten, das zu dem Terminal lieferbar ist. Durch die erfindungsgemäße Speicherung zumindest eines Teils eines Algorithmuscodes in dem flüchtigen Speicher (130) des Sicherheitsmoduls (100) wird der Algorithmuscode des Sicherheitsmoduls (100) wirksam vor einem Ausspähen durch einen potentiellen Angreifer geschützt.

Figur 2

Bezugszeichenliste

10	Chipkarte
20	Terminal
100	Chipkarte
110	Datenschnittstelle
120	Energieschnittstelle
130	RAM
140	Prozessor
150	ROM
200	Terminal
210	Datenschnittstelle
220	Energieschnittstelle
230	Prozessor
240	Speicher

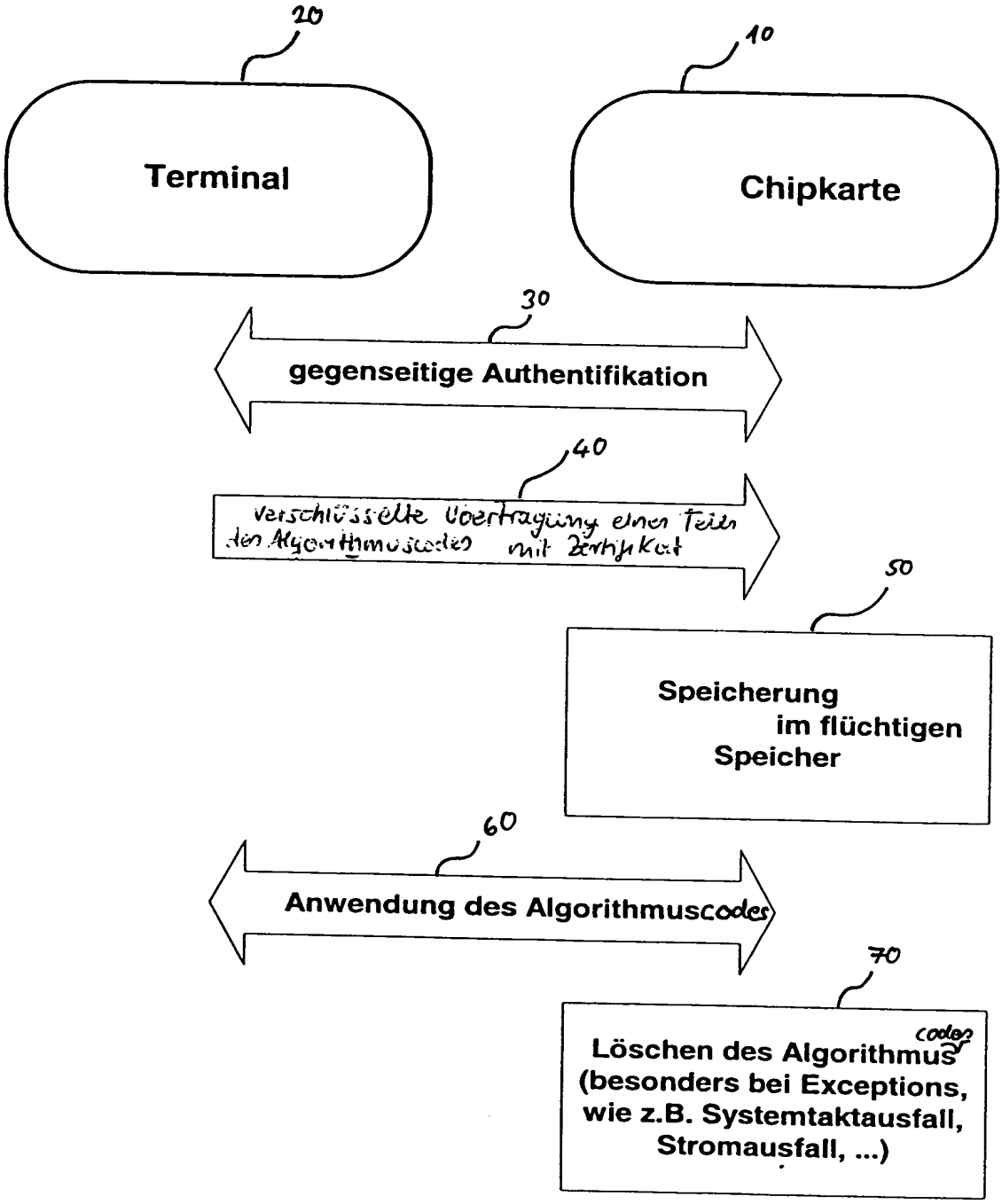
20
10
Terminal
Chipkarte
30
gegenseitige Authentifikation
40
verschlüsselte Übertragung eines Teils des Algorithmuscodes mit Zertifikat
50
Speicherung im flüchtigen Speicher
60
Anwendung des Algorithmuscodes
70
Löschen des Algorithmuscodes (besonders bei Exceptions, wie z.B. Systemtaktausfall, Stromausfall, ...)

Fig. 1

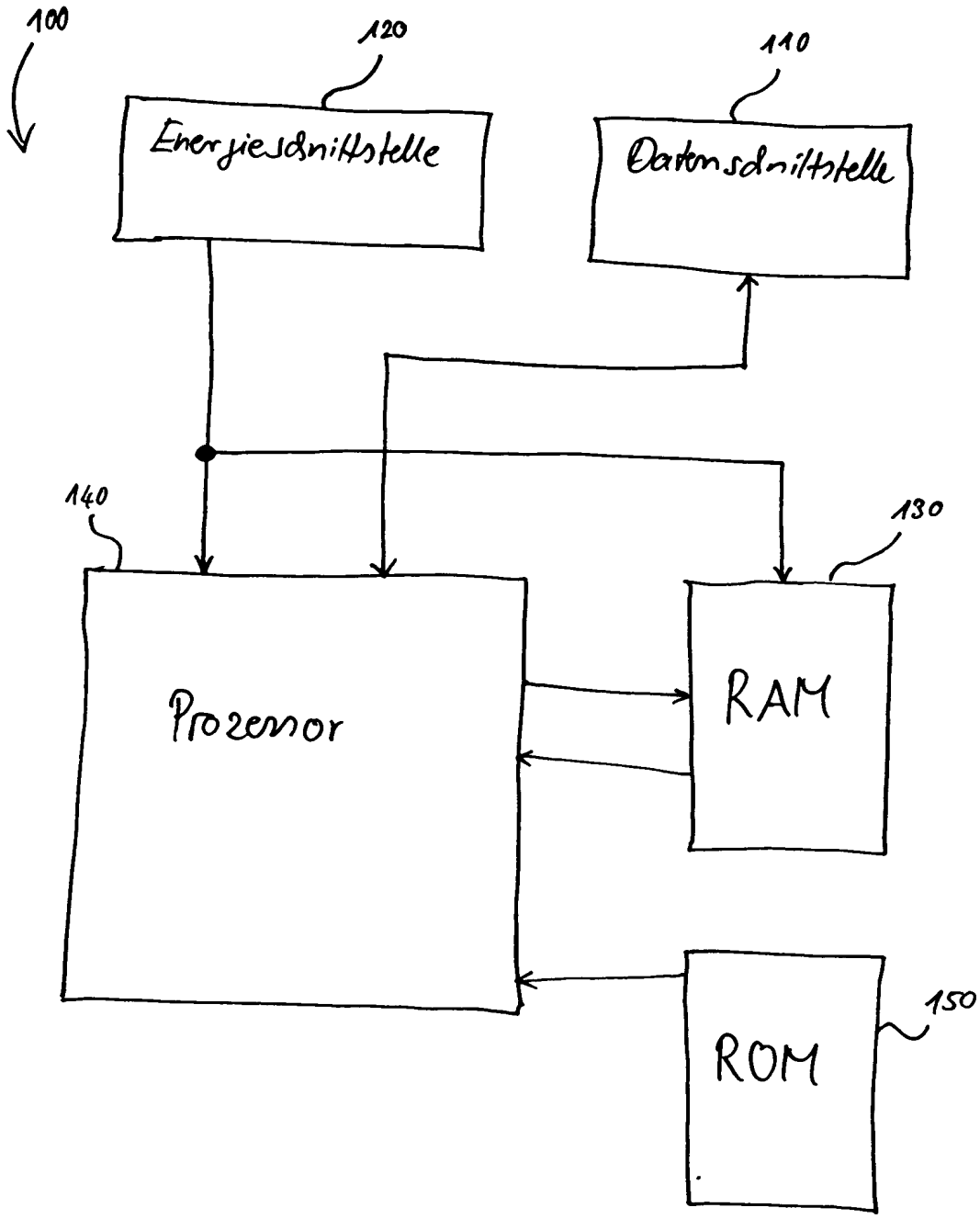
100
120
Energieschnittstelle
110
Datenschnittstelle
140
130
Prozessor
RAM
ROM
150

Fig. 2

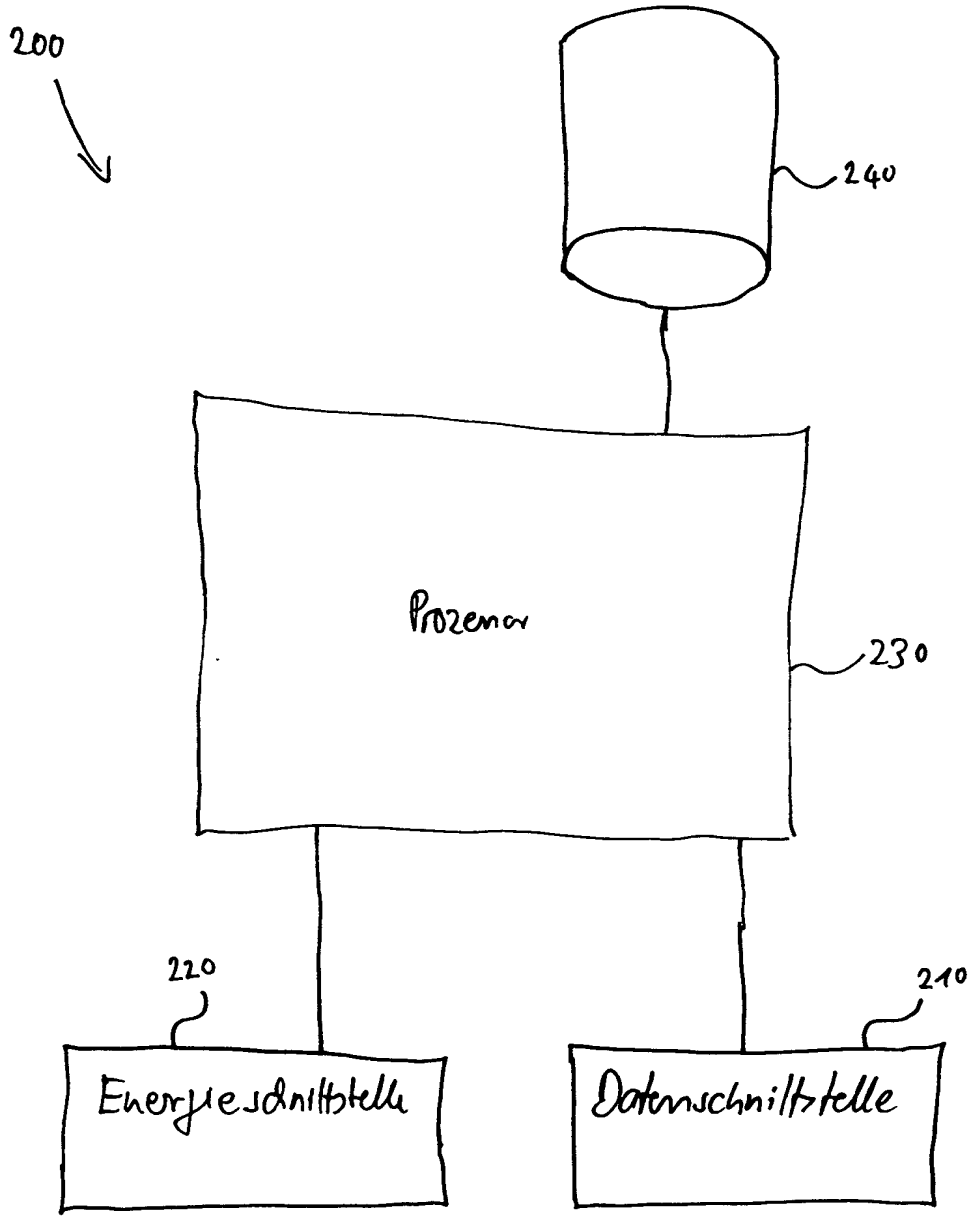
200
240
Prozessor
230
220
210
Energieschnittstelle
Datenschnittstelle

Fig. 3